出國報告（出國類別：開會）

2019 年 IIA 國際內部稽核研討會

（2019 IIA International Conference）

服務機關：台灣中油股份有限公司檢核室
姓名職稱：陳嵐嵐 稽核師
派赴國家：美國
出國期間：2019/07/05-2019/07/12
報告日期：2019/08/07

摘要

本次研討會安排將近 70 場研討主題，除了大型 keynote speeches 外，特就公司業種選擇參加主題，內容涵括舞弊侵占型態辨識技巧、組織文化氣候監測、運用科技偵測舞弊、浪費及濫用、如何運用及改善資料分析程式架構、風險評估的風險、第三方合作夥伴風險管理策略、舞弊風險評估後的下一步等，經匯聚主題重整後，分析出稽核業務的兩大支柱架構－風險評估及管理架構和稽核範疇架構，提供稽核工作者在稽核地圖上的定位指引，並於報告中再細部介紹各階段稽核工作可供借鏡之技巧工具等，供有興趣進一步結構化執行稽核任務的讀者一窺國際方法理論最新趨勢走向。

目次

壹、 出國目的

國際內部稽核協會(IIA)及國際內部稽核協會亞洲聯盟(ACIIA)為有效提升各國內部稽核人員之專業核心技能，並宣揚其於公司治理之重要性，每年皆會舉辦國際性研討會，邀請國際上相關領域卓有貢獻之公司高階主管人員及學者專家們，藉由研討會進行稽核經驗分享與專業新知之傳達，提升稽核功能以協助全球企業制度化內部治理，增加組織風險耐受能力。

貳、 研討主題總覽及報告架構

本次研討會安排將近 70 場研討主題，除了大型 keynote speeches 外，其他同時段內安排 8 場小型研討會，囿於每場次時段僅能擇一主題參加，其他主題僅能大略瀏覽簡報內容，場次擇選上儘量就本公司業種、組織型態進行主題篩選，經排除同時段簡報內容較空泛、金融業、政府公部門、外部稽核操作等實用性較低主題，本次參加主題涵括舞弊侵占型態辨識技巧、組織文化氣候監測、運用科技偵測舞弊、浪費及濫用、如何運用及改善資料分析程式架構、風險評估的風險、第三方合作夥伴風險管理策略、舞弊風險評估後的下一步等，本報告採所有主題整合後萃取精華方式重現，不就個別主題逐一介紹，經揉合所參加場次主題自建二大架構(**風險評估及管理架構和稽核範疇架構**)，建立架構之目的在於協助讀者釐清從事稽核工作之意義與目的，綱舉目張下清楚自身在稽核地圖上所處的定位，並以風險導向精神一以貫之，免得在茫茫稽核事務中迷失方向，再針對架構下各項細部工作研討會內容作進一步闡述，供有興趣結構化執行稽核任務的讀者一窺國際方法理論最新趨勢走向，不免有筆者檢視本公司現況所作出的比較分析，筆者建議閱者仍應經過獨立性思考檢視，並因地、因人制宜，找出屬於公司的最佳解決方案。

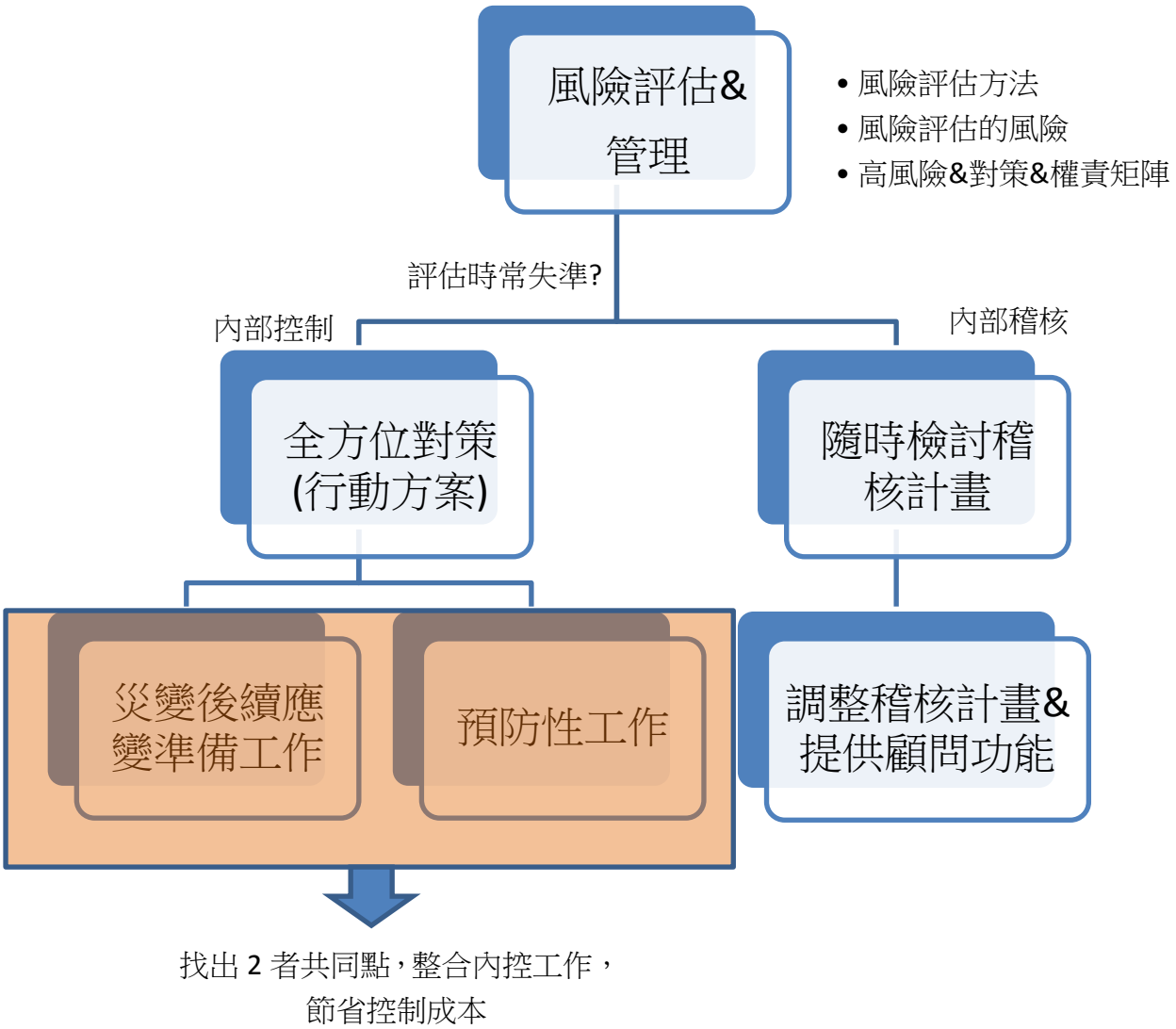
由於架構(研討心得)與各類主題介紹具上下關聯性、交互穿插難以拆分，本報告將研討會重點及心得分享整合於同一區塊統整介紹；另外值得一提的是大型 keynote speeches，大會邀請分享對象通常非稽核領域專家，旨在提供與會者跨領域思考刺激，而其中一些講者身分亦看得出工作型態轉變新趨勢，其分享內容則有助於提升個人面臨職涯風險之應變能力，將置於本報告第參之三要項作簡單

分享。

日期/時段	參加之研討會/工作坊主題名稱	類別性質與內容
7/7	報到及主題挑選 workshop	報到及研討會主題介紹
7/8	GS 1: A Violation of Trust: How Bernie Madoff Changed a Nation — Fireside Chat CS 1-2: Auditing and Monitoring an Ethical Culture CS 2-2: Case-based Learning — How to Identify and Defeat Newly Identified Complex Embezzlement Schemes CS 3-4: Case-based Learning — Leveraging Technology to Detect Fraud, Waste, and Abuse CS 4-3: The Risks in Assessing Risk GS 2: Dynamic, Disruptive Diversity: A Bold Approach to Harnessing the Power of Differences	－《龐氏騙局》與稽核職責 －道德及守規性組織文化氣候監測與維持 －舞弊案件特徵與破解對策 －奧勒岡州透過資料分析找出補助冒領案例分享 －風險評估的風險（盲點） －多樣性觀點與自我潛能開發
7/9	GS 3: Performance Excellence: The Employee Factor CS 5-4: How to Use and Improve an Audit Data Analytics Planning (DAP) Framework CS 6-3: Effective Anti-bribery and Anti-corruption Programs: Applying Risk Management Strategies to Third Parties CS 7-2: You Completed a Fraud Risk Assessment: Now What Do You Do? GS 4: Geopolitics and the Global Economy	－迪士尼經營成功秘訣 －稽核資料分析程式架構(DAP)與思考工具 －風險評估及管理、第三方合作夥伴風險管理 －風險辨識、評估及後續控管 －全球政經情勢分析
7/10	GS 5: Leadership Panel Discussion: Challenges, Opportunities, and the Path to Success GS 6: Reinventing Leadership for the Age of Machine Intelligence 頒獎與閉幕式	－三位女性總檢核座談分享成功經驗 －未來 AI 世代來臨產業樣貌變遷及因應思維

參、 2019 國際稽核研討會心得及重點整理

一、 風險評估及管理架構



（一） 架構說明

坊間有許多辨識風險、風險評估的理論方法，但再多的理論仍無法避免風險值誤判，尤其身處速變時代，許多風險是預測不到的，所以風險評估失準情形時常發生，組織面臨總是測不準的風險，既然無法阻止風險發生，最好的應對方式

就是做好萬全準備，凡事應有最壞打算，並針對各種情境擬定全方位對策，從對策再衍生各種行動方案，平時將這些行動方案落實執行，這種觀念極類似現行的內部控制制度(以下簡稱內控制度)，雖然每間公司都有內控制度，但內控制度的周延性、落實性卻大大影響其風險防範效果，在研究各種行動方案時應該同時考慮二種面向，其一是預防性工作，也就是預測風險，並趕在風險發生前就做好因應對策，根本杜絕風險發生；其二則是災變後續應變的準備工作，風險總有無可避免發生的時候，當各種等級的風險確實發生時，組織內相應的災變通報、處置、善後等工作作業程序是否存在、適度發揮效用?是否有落實演練? 所以吾人可以從這些角度去檢視現行的各類內控制度，朝更加周延、更加完善的方向去努力改進內控制度。

站在稽核的角度而言，風險評估是稽核計畫根本，如今面對變化莫測的經營挑戰，遂發展出迅捷稽核計畫趨勢，稽核計畫仍應保有彈性空間，因應組織環境需求適時做出調整，或輔以專案查核計畫以補強週期性稽核計畫的不足。

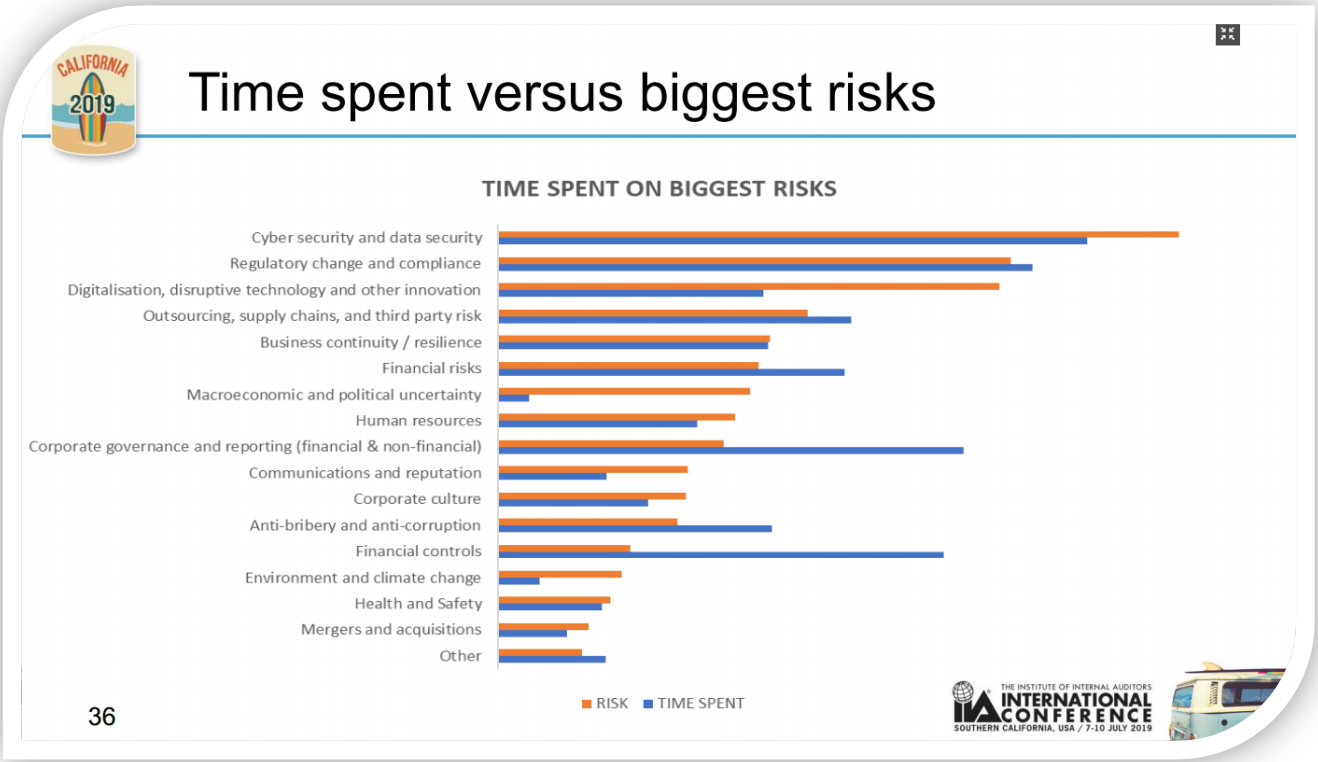
(二)2020 年稽核熱門議題(簡報重點摘錄)

本次研討會有一場研討主題與未來稽核重點發展有關，專家介紹國際稽核預測 2020 稽核熱門十大議題排序如下表，並選擇部分重點項目進一步說明稽核新趨勢以協助企業，並提醒各稽核人員調整稽核方向。

排序	風險	稽核新趨勢
1	資訊安全及資料保護	針對提供服務的上游公司進行聯合稽核，例如使用 Amazon 雲端倉儲服務的各家銀行組成聯合稽核團隊
2	日益增加的法令遵循負荷	---
3	數位化及商業模式創新破壞	1. 檢視專案計畫是否符合企業策略方向 2. 專案控制，留意是否落實變動管理 3. 評估專案風險 vs. 效益，是否值得執行?
4	第三方管理	---

5	企業復原力、品牌商譽價值	預防性：留意重要營運風險、評量預防意識強度 偵測性：早期發現事件徵候、損害控制
6	財務風險(舉債獲利壓力)	---
7	地緣政治不穩定&總體經濟	外部風險因應： 1. 組織有正確消息來源、正確因應行動，以早期發現風險? 2. 若萬一發生，組織能快速因應? 3. 各相關營運面向是否得到適當控制?(衍生性商品交易、營收預測、供應鏈管理…等)
8	人力資源(未來的組織面貌)	1. 評估招募方式是否仍有效?(吸引 z 世代) 2. 職場環境應該有什麼調整? 3. 哪種組織模式最能符合策略方向? 4. 若選擇某種組織模式，內控需要做哪些改變?
9	企業、道德及文化(模範組織)	1. 透過訪談、問卷、觀察等觀察組織氣候 2. 風險所在：組織未落實或欠缺對付壞份子的措施
10	氣候變遷(風險 vs. 機會)	外部風險因應： 1. 組織有正確消息來源、正確因應行動，以早期發現風險? 2. 若萬一發生，組織能快速因應? 3. 各相關營運面向是否得到適當控制?(衍生性商品交易、營收預測、供應鏈管理…等)

這份簡報中還有一項有趣的統計,有關於風險大小 vs. 投入的時間(如下圖),會發現很多不成比例的地方，譬如組織花了許多時間在預防財務風險，然而該項可能是風險相對較低的項目，而總體經濟風險影響企業雖大，但組織投入預防的時間卻是相對很少的，許多企業或許認為總體經濟或地緣政治屬不可控因素，企業難以準備故投入最少，但如果一旦發生此風險卻可能導致企業周轉不靈倒閉，企業如能事先做好組織復原力檢視及準備，也許就能撐過下波巨浪來襲。



(三)風險管理與稽核計畫

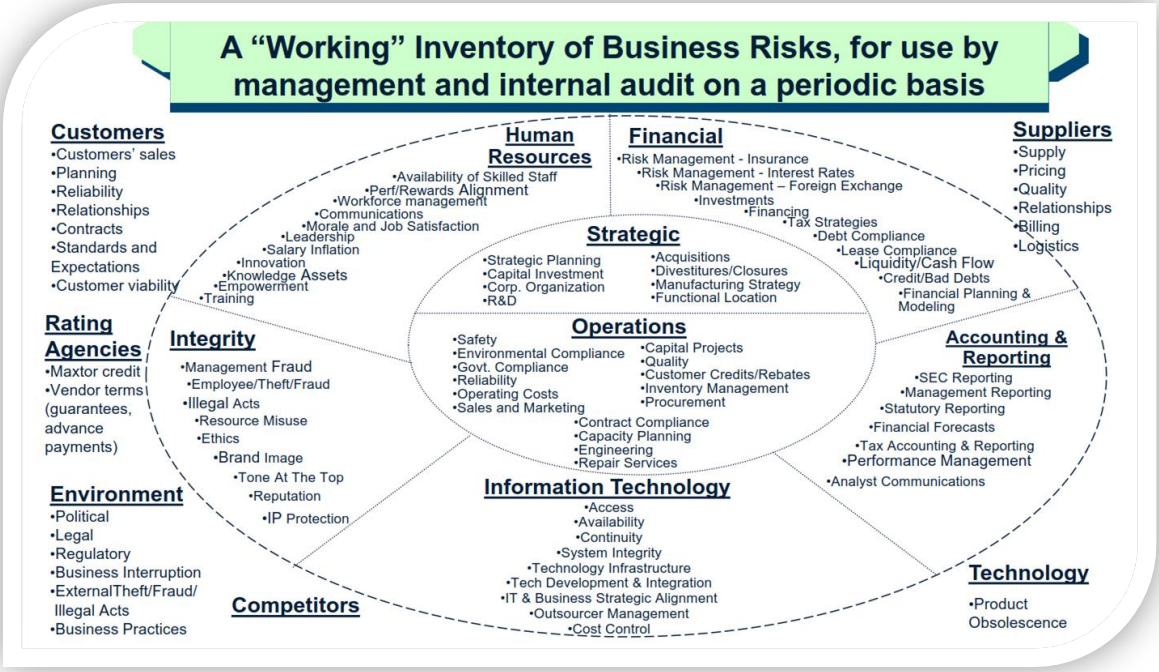
在開始擬定稽核計畫前,應先關注董事會、主持人、單位主管所在意的風險,譬如營收或獲利目標、市占率、大型專案、聲譽等,因此稽核應該先從了解企業開始,組織目標為何?這些組織目標面臨什麼樣的風險? 哪些風險可能馬上發生?專家建議可從以下幾點去思考:

1. 哪些事情會讓老闆半夜驚醒?
2. 哪裡可能出錯?
3. 哪些做對了?
4. 你把時間花到哪去了?
5. 你的目標是否處在風險中?
6. 董事會議程重點是哪些?

下一步就在於如何偵知風險,可透過以下幾個管道篩選:

1. 企業風險管理 ERM(Enterprise Risk Management)
2. 老闆、主管訪談
3. 營運報表
4. 小組討論
5. 內部稽核腦力激盪(模擬情境)
6. 平時蒐集觀察
7. 平時閱讀各類文件報表及研析
8. 外部稽核報告

專家建議可以建立企業風險智庫，例示如下圖，做為定期風險評估時之參考：



本公司目前從事的諸多內部控制事項均在上圖可稽，例如營運方面第一項風險即為工安環保、法令遵循等，風險智庫有助於健全風險管控面向，有些更為重視的公司，其風險智庫以矩陣呈現，明確定各項風險、因應行動方案、權責分工等。所以整體風險管理流程可歸納如下：

1. 使用工具找出控制範疇及架構
2. 根據公司環境模擬風險情境
3. 評估風險發生可能性及衝擊度
4. 媒合各項風險與現有內控制度
5. 指定各項內控權責

6. 適切的管控強度
7. 找出內控不周延之處，評估是否納入內控
8. 風險評估結果溝通

在根據風險評估結果制定稽核計畫之後，須注意稽核計畫之制定是否能立即回應企業營運所需，此即牽涉到稽核計畫檢討週期，迅捷的稽核計畫會跟隨企業腳步及風險變化速度更新，在本公司(除一般年度實地查核計畫)此部分應係透過專案稽核補強，但專家特別**強調根據風險評估的稽核計畫很有可能只是在解決昨日問題或挑戰，並無法做到預防性稽核**，這是大多數公司內部稽核的盲點，套句冰上曲棍球選手 Wayne Gretzky 說的話：「一些人滑向冰球，而我滑向冰球會溜去的方向」(“Some people skate to the puck. I skate to where the puck is going to be.”)，為了做到預應式稽核，專家建議以下幾種自我精進方法：

1. 傾聽
2. 閱讀管理報表
3. 閱讀產業新聞
4. 深入現場
5. 管理議程重點有哪些?
6. 董事會議程重點是哪些?

有好的報告就需要好的向上溝通，要考慮高階主管速動日程，務必去蕪存菁，也可以透過多層次溝通達到溝通效果，報告文字切忌冗長，只寫自己想寫，忽略讀者需求，或把稽核報告當作流水帳紀錄浪費彼此時間，或將珍珠藏在垃圾山裡都是無效的溝通。然此點在實務上仍有執行彈性，在本公司為證明確有扎實辦理實地查核，稽核人員均戮力撰寫報告，導致報告內容較為冗長，然檢核室亦有考量高階主管時間有限，故發展出「摘述報告」，要求稽核人員篩選重點缺失項目，俾減輕主持人及獨立董事閱覽負擔，確保重點一目瞭然，不失為一替代方案，但專家建議仍值得各級稽核人員參考，**報告描述力求精簡切中要害可作為共同努力目標**。

本節以加州知名顧問公司 Protiviti Inc. 名言共勉：

內部稽核真正的價值不在於事後成堆的建議，而是能提供及時建議及引導正向改變。

"The true worth of internal audit is not measured in the weight of after-the-fact recommendations, but in the ability to provide just-in-time advice and influence positive change."

(五)風險評估的風險

這場研討會的取名有點耐人尋味，我們日常常在進行的風險評估工作本身可能就存在著誤判的風險，也可以說是風險評估的盲點，一般人評估風險時只評估災損，但風險不僅僅如此，風險=(風險災害+失控的人心)X 社群媒體，也就是說風險很多時候會因為人們驚慌失措及社群媒體散布恐慌而讓災害擴大。專家用了以下一些例子及心理學理論來提醒我們風險誤判的情況確實存在：

1. 搭飛機風險比開車來得高? 實際上若訴諸統計數據，就會發現搭飛機出事的可能性遠低於自駕，美國國內平均搭機(694 英哩)事故風險=在洲際高速公路開 10.8 英哩的路程風險，那究竟是什麼影響到我們的判斷? 也許是空難事故新聞更令人印象深刻，另外一點也許是因為自駕你擁有控制權，但搭飛機你只是個被動的乘客，所以人們傾向相信擁有掌控權風險會比較小。
2. 控制權究竟有多重要? 一項簡單的實驗讓大家看看控制權的重要性，將護理之家的病人分成兩群，實驗組可以自己決定房間擺設、選擇想要照顧的盆栽等，而對照組則是被動接受一切，房間已經被布置好、盆栽也是被指定照顧的；18 個月後觀察死亡率，發現實驗組死亡率 15%，對照組死亡率則是 30%，所以**相信控制權能降低風險的想法並不全然是錯的!**
3. 人們傾向找出模式(pattern)。這種傾向其實源自於演化，找出壞徵兆模式讓我們生存下來，但**實際上一切也許只是雜訊，根本不存在所謂的模式**，只是人們寧願誤判信息也不能有個萬一，而賭場深知此心理，於是他們在顯示幕上動手腳，讓你誤以為賠率或輸贏其實是有模式可循的，即便是蘋果也修改 ipod 隨機播放功能，讓它不那麼隨機，好讓消費者相信它是隨機的。
4. 你真的能預測機率嗎? 如今兩盞燈擺在眼前，一個紅一個綠，二者隨機閃爍，但紅燈閃爍的時間佔 75%。如今邀請你跟一隻老鼠進行比賽，猜測下一次閃爍到底是紅燈或是綠燈，你有二種策略可以選擇，其一是一直選紅燈，其二是

猜測二者閃爍機率，實驗結果很可能是老鼠贏了，因為老鼠沒想那麼複雜，只會一直選紅燈，所以成功率是 75%，而人類傾向猜測機率，成功率約 60%，其實不用沮喪，這跟人的大腦構造有關，人的右腦傾向模式思考猜測，左腦則傾向猜測較常出現的顏色(相信隨機)。

5. 你真的可能被誤導。

   －案例一：以下二種情境，你覺得何者較可能發生?

   (1) 北美某處一場致命性土石流導致數百人喪生

   (2) 加州地震導致的一場致命性土石流導致數百人喪生

   答案是(1)，你猜對了嗎?

   －案例二：Linda 是個 31 歲、獨身、外向又開朗的女性。她主修哲學，身為一個學生她十分關注種族歧視及社會正義，她也參與反核示威遊行。以下何者可能性高?

   (1) Linda 是個銀行員

   (2) Linda 是個銀行員，而且她活耀於女性運動

   答案是(1)你猜對了嗎?

   從以上二個例子可以知道人們傾向找尋跡象解釋一切，而故事性描述較一堆隨機事實陳述來得容易記住，而凡此種種都容易讓我們**被事情描述方式誤導**。

6. 後見之明偏誤 (Hindsight Bias)。指當人們得知某一事件結果後，誇大原先對這一事件的猜測的傾向，俗語稱「**事後諸葛亮**」。 後見之明偏見的一個基本的例子是，在知道一個不可預見事件的結果後，一個人相信自己「早就知道結果會這樣」，實際上許多徵兆在事前被忽略，導致 911 事件、珍珠港事件等。後見之明的偏見**可能導致記憶失真，回憶與重建內容時產生錯誤的理論成果**。譬如問你 6 個字母的單字中第 5 個字母是 n 的比較多，還是結尾是 ing 的比較多，你很可能回答 ing 的比較多，但實際上卻是另一個比較多，等你知道了答案之後才會開始細想。

7. 可得性偏差 (Availability Bias)。可得性偏差指的是我們更容易被自己所看到或者聽到的東西影響，而**不是用統計學知識去思考問題**。

8. 錨定謬誤 (Anchoring fallacy)。欠缺客觀標準下，我們傾向找尋可得的標準。也就是說為不熟悉事物估值時，會把熟悉的類似事物或不久前接觸到的**無關數值**當做「錨」，估出來的數值會大大傾向「錨」。譬如叫觀眾先寫下身分證末四碼，接下來請觀眾估測在曼哈頓的餐廳有多少家時，觀眾猜測數字

通常跟身分證末四碼有關。

9. 後悔趨避傾向。如果你去電影院，現在正辦理一個活動，A.前 10 萬客戶可以贏得 USD100，B.第 100,001 的客戶可以獲得 USD150，你會想選擇哪個? 機率計算下大多數人會選擇 A，因為他們怕會後悔自己的選擇。
10. 同儕偏誤（Voice bias)。不可否認的我們的決策很容易受同儕影響，就像共和黨員傾向支持共和黨提案，無論那提案是否顯得很民主黨色彩。
11. 肯證偏誤（Confirmation bias)。人們傾向相信自己的判斷正確，無論事實證據擺在眼前多麼明顯，而且人們討厭承認自己會犯錯，所以走進此演講廳的聽眾應該都覺得這場研討會如同自己想像的好(或差)。
12. 權力矛盾（The Paradox of Power)。研究顯示所有那些推升你成為領導者的美好特質終將逝去，權力讓你變了個人，從誠實、禮貌及外向轉變成任性、膽大妄為及粗暴。當人們抵達權力頂峰時傾向仰賴過去成功經驗、以成見歸類其他人、比以往更少眼神接觸、欺騙及合理化自身行為。請不要難過，這是人腦及基因所致。

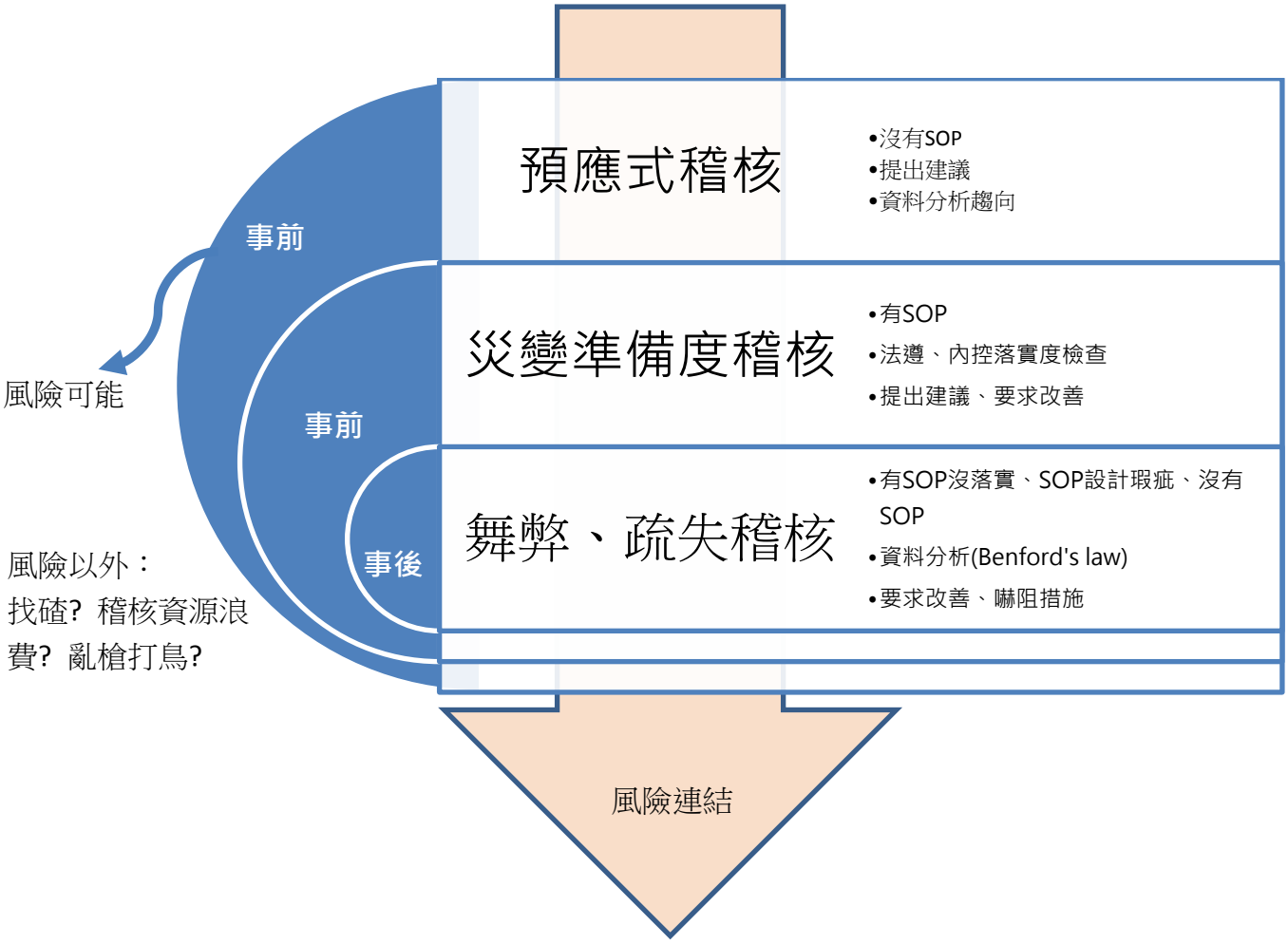
看完這些那我們到底能怎辦? 專家建議下列幾項注意事項，有助於我們遠離各式各項的偏見：

1. 確定你真的了解風險可能性是什麼(不是自己猜的)。
2. 承認即便我們知道風險是什麼，也不意味著我們會依照認知行動。
3. **真正的風險會因為失控的人而被放大**。
4. 承上，風險強度也會被事件戲劇性程度影響，且易被憶及。
5. 別被「模式」牽著鼻子走。
6. 牢記所謂的隨機看起來可能並不隨機。
7. 留意可得性偏差。
8. **我們對風險的認知可能受「誰」做風險評估影響**。
9. 別被錨定謬誤絆倒了。
10. 留意你的描述方式。
11. 即便掉入後悔趨避陷阱，也不用感到後悔。
12. 注意肯證偏誤。
13. 像個興業家一般思考（將風險與機率一起考量)。

除了這些之外，既然人們無法精準預測風險，唯一的辦法就是做好萬全準備，

你無法控制風險，但至少你能控制反應，制定一套具備彈性的應變資源，在各種應變解決方案中**找出共同性**，好**以最少的成本做到風險控制**。

二、 稽核範疇架構



(一) 架構說明

稽核工作最大目的在防範風險發生，或確保風險發生時組織已做好應有的準備，加速組織復原速度，此外若發生舞弊或重大疏失事件時稽核介入調查也在於發掘真因，以便彌補內控漏洞防範風險再度發生，所以一切稽核工作都與風險密不可分，從事稽核工作時應時時捫心自問目前查核項目是否與企業風險確實相關? 若**此項缺失改正與否並不影響營運風險程度**，則可能落入所謂找碴、亂槍打鳥之盲點，徒浪費組織稽核資源。

如果以風險發生做為切割點，則稽核工作可區分為事前防範及事後改正。事前防範又有二種層次，其一為預應式稽核，透過資料分析、實地觀察等方法發現趨勢，及早提出改善建議，以預防組織遭遇風險事件，通常會發現內控制度的漏洞、欠缺 SOP 的作業環節，屬積極面作為，但也容易遭質疑建議妥適性；其二為災變準備度確保稽核，屬消極面依照現有制度 SOP 進行逐項檢點檢視，有一種說法就是 checklist 方式稽核，也適用法令遵循檢視，通常會納入法規的作業規範即表示該工作項目具備相當程度風險，並已廣為人知，所以針對法規、SOP 進行 checklist 稽核，旨在檢視組織面臨已知風險的準備程度，這些已存在的 SOP 可能包含預防性措施及災害應變措施(含演練)，**筆者觀察此類目前占去大部分稽核工作。事後改正部分常見於重大疏失、舞弊事件查核，一般以專案查核方式進行**，此類查核目的有二，其一為改善風險內控制度，彌補漏洞防止再發生；其二則是責任檢討，以嚇阻再犯；由於部分非尋常案件偵測初期犯案手法未知，稽核人員會運用一些統計分析工具如班佛定律(benford’s law)找出高度疑點標的，好聚焦縮小偵查範圍，俾便早日釐清案情，並提出改善建議。

(二)　組織文化氣候監測(含第三方管理)

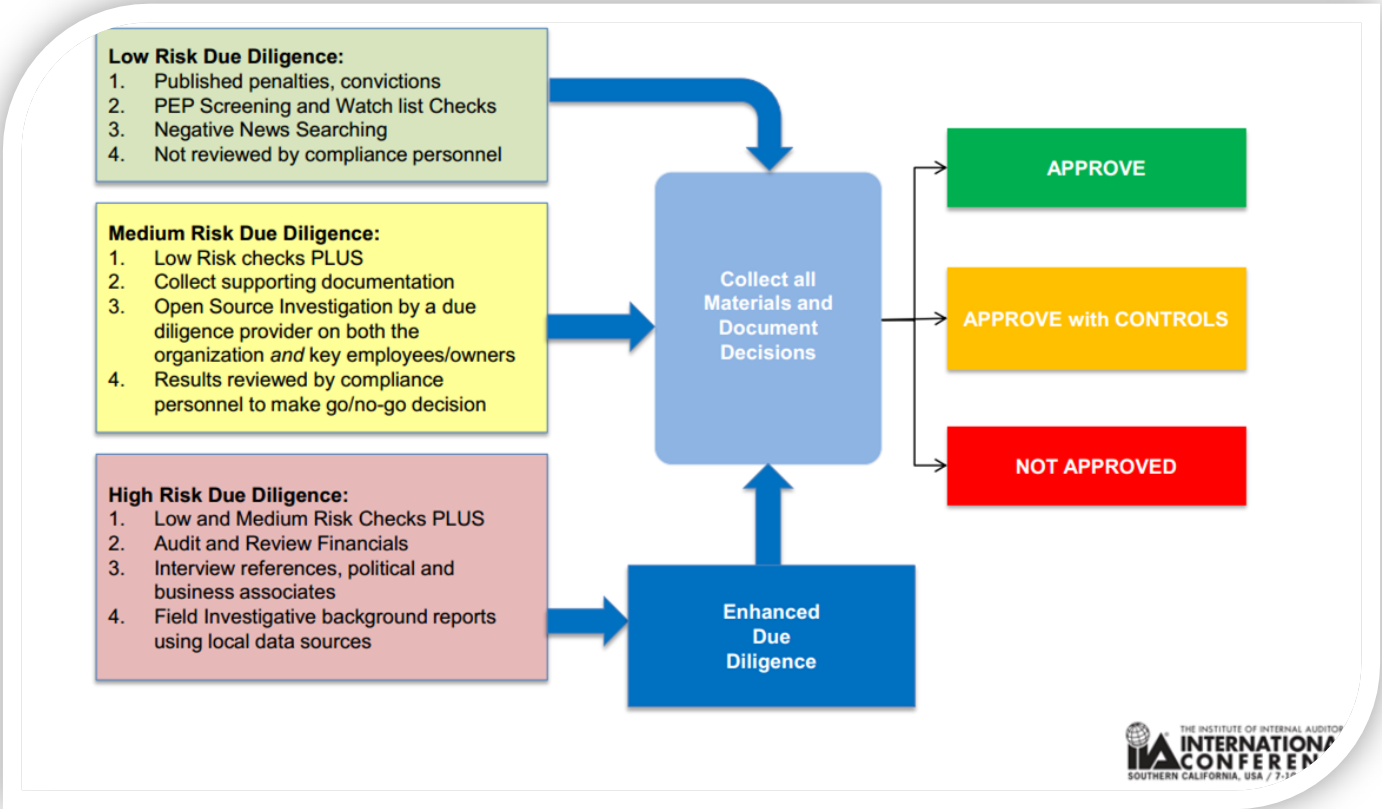
所謂的風險評估、稽核計畫擬定、資料分析稽核、稽核報告撰寫溝通等技巧在稽核領域來說都屬於術的應用，大家都曉得**最好的稽核並不在於查出多少缺失，提出多少改善建議**，而是在於**成功營造誠實守規的組織氣候，從根本根除違犯行為**，這才是真正成功的稽核功能發揮，於是如何監測組織氣候，塑造人人守法、隨時防範風險意識的文化也成為本次探討的主題之一。專家建議從 9 個面向(如下圖)去共同促進，而稽核人員則是定期進行 9 面向落實程度檢視，以確保組織氣候持續維持一定水準，這 9 個面向分別是公司核心價值、員工行為守則、風險評估、風險對策及相應賞罰程序、道德守規意識訓練、多元溝通宣傳管道、詢問及通報機制(設置熱線?)、定期評估並檢視程序、主持人支持程度。

話雖如此，如今許多公司將部份工作外包給第三方廠商代辦，**這部分佔比逐漸擴大到不容忽視的地步，第三方管理儼然成為目前最頭痛的項目**，許多第三方**合作夥伴常違規行事，讓企業暴露在未知風險中**，企業如何善盡善良管理人義務已成為必須面對的課題，本次研討會中有專家提出初步做法供與會者參考，公司須於契約中明定第三方責任義務，明訂公司介入時機，公司本身須有承攬商管理標準，並明確告知第三方公司內、外相關法令遵循義務，**不僅僅止於告知，還必須透過查驗確保第三方遵循程度，並應留存通知抵達紀錄**，另一項比較困難的是**公司是否有整合與外部間的管理介面**。下表顯示第三方風險因子及因應對策，或有助啟動讀者外包商管理的思考起點：

第三方風險因子（依不同對象自行評估排序）	第三方風險管理對策
▪ 財務穩定性 ▪ **過往承作歷史** ▪ 第三方據點地理分布	▪ 在整個履約生命週期採分層管理方式管理風險 ▪ 第三方教育訓練

▪ 契約價值及履約期間 ▪ **過往違犯前科** ▪ 再轉包商關係 ▪ 過度折價及利潤管理費 ▪ 存續性風險 ▪ 機敏資料取得性 ▪ 支援組織關鍵性業務	▪ 將整個履約過程嵌入公司各個部門作業(如契約、稽核、採購、訓練、財務等) ▪ **將當責及指揮監督推導融入** ▪ 透過報告及報表進行資訊共享 ▪ 分析第三方員工群體為企業提供加值服務

此外，第三方合作夥伴的背景調查也不能輕忽，根據各種檢查點檢視結果，決定採取合作、有限度合作、拒絕合作等決定，檢查點及決策流程請參考下圖。



簡單來說，低度風險檢查包括了過去不良紀錄、政府採購停權名單、新聞蒐集等，而進階到中度風險檢查時，除了低度風險檢查點外，又增加了企業或員工背景調查、法遵人員檢視結果等，高度風險檢查則又再增加企業財務稽核檢視、工會團體口碑調查、運用當地資料進行背景田野調查等。這些調查結果匯集供公司參考是否願接納該第三方成為合作夥伴，或者是輔以有限度控制措施進行合作，**如果諸多資料顯示有問題，則最好是拒絕往來以降低公司暴露風險**。

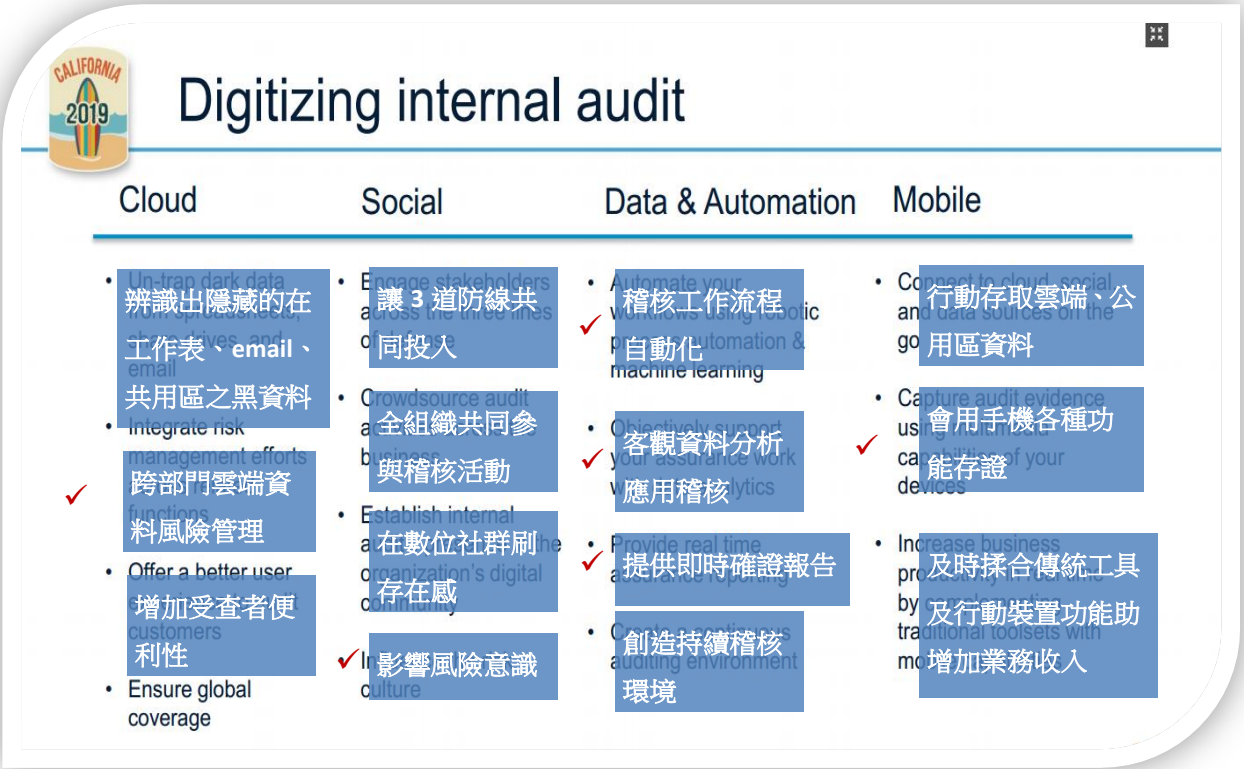
（三）　稽核文化地雷(簡報重點摘錄)

由於不清楚稽核工作本質，常見組織誤踩之稽核文化地雷如下：

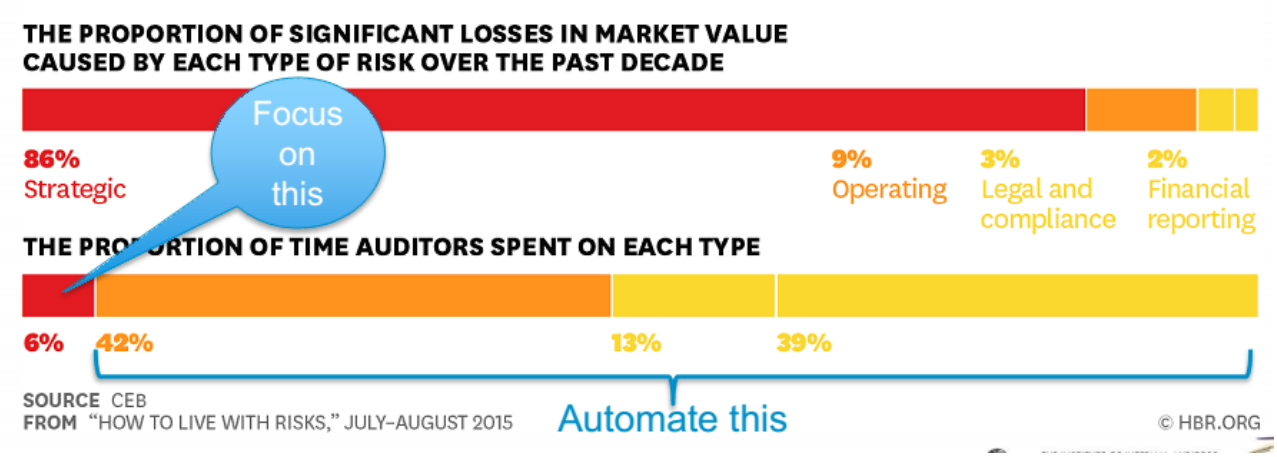
1. 追求短期利益(如財務上、政治上)，包含個人利益，忽視客戶(社會)關注價值
2. **過度重視政治正確，而非經營績效目標**
3. 拘泥於法規文字，忽視立法精神、以法無明定作藉口選擇性辦案
4. **視風險評估程序為麻煩事，必要時可以權宜省略**
5. 無法清楚**定義風險管理權責劃分**
6. 無法對好的風險管理做出正面回饋，或助長差勁的風險管理措施
7. 高階主管未採取及時行動以降低重大風險
8. 掩蓋問題，而非找出並解決問題背後的根因
9. **怯於挑戰現況或考量替代觀點**，導致耽於組織安全幻覺、暴露在風險盲點中

（四）　數位化破壞式創新之於稽核(簡報重點摘錄)

讓我們來檢查一下本公司稽核數位化上是否跟得上國際潮流吧！以下打勾者為筆者認出本公司部分應用數位科技推行之項目，顯示其實數位稽核仍有挺大的發展空間。



據研究顯示，企業承受損失中占比最高者來自於決策風險，其餘依次為營運風險、法遵風險及財報風險（如下圖表），若能透過數位化管理營運風險、法遵風險及財報風險，則能投入更多精力提升決策品質。



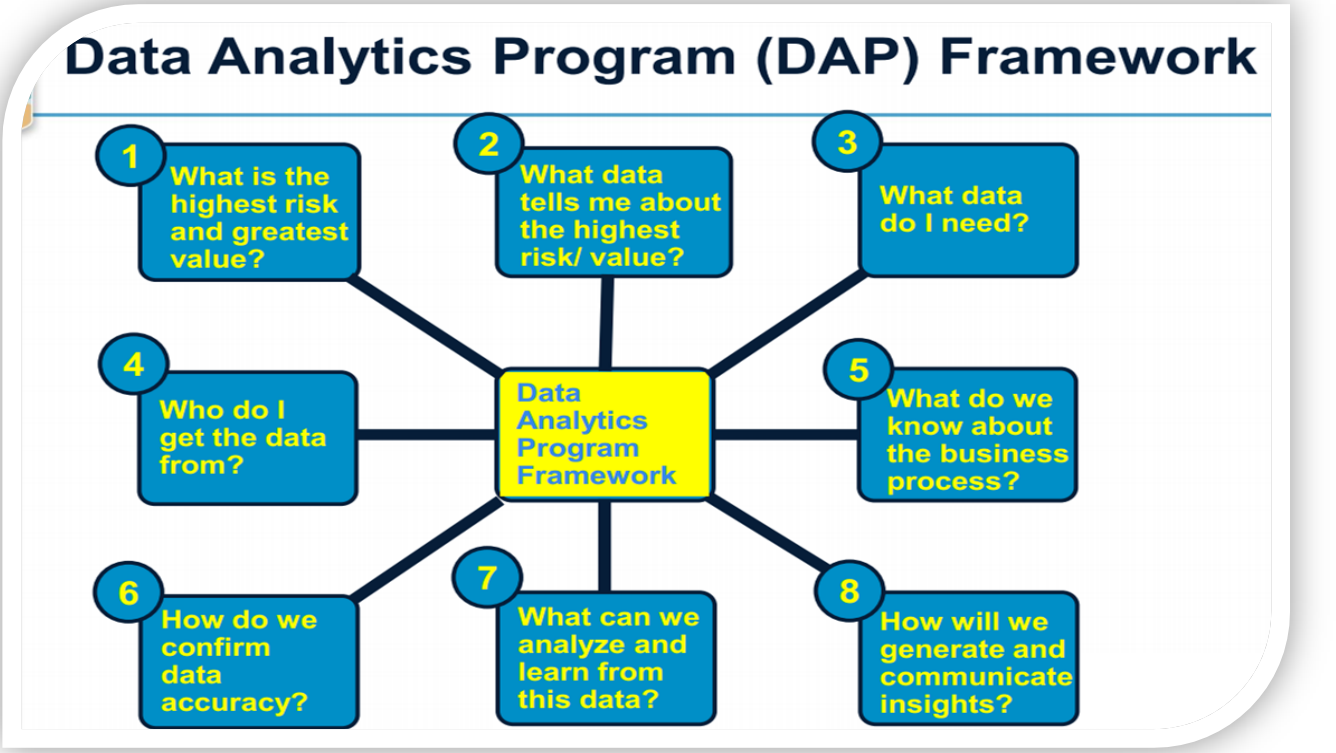
除了稽核資源配置考量外，數位化管理也有助於決定解除追蹤時機，透過系統即時更新各風險項目缺失發生頻率及重新計算改善後殘餘風險值等，當風險值降至控制目標後，則可解除追蹤。數位稽核的終極應用為發展大數據預測模型，以大數據分析過往缺失模式，找出例外、異常情境的特殊早期跡象，發展預應式風險模型，早期偵知、預測並預防高風險情境發生。

面臨人工智慧浪潮來襲，未來稽核職能需求也開始產生變化，稽核人員可能要開始發展諸如 1.數據科學(包含偵知、預測、預防、甚至是風險容忍度之資料分析)2.行為科學(有助於決策或風險評估的「行為經濟學」漸夯)3.數位學養(利用系統、網路、行動裝置等管理風險及內控)等職場技能，**積極面來看，自動化並不意味著取代工作，而是將人類工作往價值鏈上端推升，為稽核騰出更多資源投入預應式工作(如組織轉化、應付新興風險等)，讓稽核成為問題解決者，而不只是問題發現者。**

(五)　資料分析稽核

其實本次研討會中有安排某些運用新科技進行稽核之主題，筆者參加其中 2 場後發現講者多半運用資料分析稽核的案例分享，或者是前端資料蒐集技巧、資料陷阱等，較少著墨資料分析方法本身，認真想想其實也是有道理的，資料分析可能涉及軟體介紹、運用、統計分析模型介紹，而這部分課題極難在短短 1 小時內進行分享，也已經涉入統計分析、資訊軟體學習應用領域，通常需要參加長期課程習得，而區塊鏈介紹對於金融業或許感受深刻，對於本公司現行實務運作上又稍嫌遙遠，故本節偏重資料蒐集技巧及案例分享介紹。

西雅圖大學 IT 稽核分析客座教授介紹了資料分析程式架構(DAP)，透過 8 種自我詰問方式(如下圖)來確定所蒐集到的資料具可靠性、具備資料價值、從中萃取有用資訊等。



專家進一步闡述這 8 個問題的思考步驟，並讓與會者親身參與小團體討論，筆者將之整理如下表，透過下表嚴謹檢視態度，將有助於提高資料分析結果準確度。

序號	問題	詰問思考步驟
1	**何者**具最高風險及最大價值?	1. 訪問高階主管、流程關鍵控制者、資料管理者 2. 「目標」常存於心，以標記出存在風險或新事業風險 3. 使用國際機構已開發模型進行結構式研討(如 APQC)
2	**那些資料**能供我辨識最高風險/價值?	1. 想想最重要的業務流程及其創價方式 2. 想創價的你需要哪些資料? 3. 捫心自問公司治理時參用那些資料來判定業務

序號	問題	詰問思考步驟
		是否成功? 4. 這份資料所衡量的標的或確認的風險層級,有符合你的稽核目的嗎?
3	我需要什麼資料?	1. 你知道這類資料的存在嗎? 你能找到它嗎? 2. 取得樣本資料或元資料(metadata) 3. 跑一些統計數據(平均數、中位數、模式分析、標準差、相關係數或迴歸分析等) 4. **確認**這資料符合我的稽核目的
4	可以從**誰**那邊取得資料?	1. 找到可以授權或提供資料給你的那個人 2. 聯繫資料擁有者、管理者、超級使用者或資料庫管理者 3. 資料清理及平準化 4. 保存及持續更新你的資料
5	我們對**業務流程**的了解程度?	1. 研究業務流程，好決定需要哪些資料 2. 取得既有資料或元資料 3. 處理資料取得限制或不正確的資料 4. 找出最高風險點或資料分類紀錄
6	我們如何確保**資料正確性**?	1. 要有心理準備此點可能是很難達成的 2. 先判定取得資料的正確(精確)程度 3. 判斷資料來源是否可靠 4. 遵循 IIA 2310(辨識資訊)及 2320(分析及評估)標準 5. 資料正確性判斷五要素：完整性、一致性(非制式資料? 矛盾資料?)、正確性、資料重複、整體性(缺少參照等) 6. 探究導致資料錯誤原因，公司或 IT 部門知道這情形嗎?
7	我們可以從此份資料裡**分析**得知哪些訊息?	1. 思考採取之資料分析方法(分類方式：主題、內容、敘述性資訊、歷史資料、業務流程) 2. 找出易於量測或量化的部分 3. 這資料可以量測或確認目標風險層級嗎?

序號	問題	詰問思考步驟
		4. 是否使用業界標準資料?
8	我們如何產出並有效溝通**見解**?	1. 提綱挈領說明資料來源及分析 2. 提出有力見解及價值 3. 圖像化溝通 4. 向利害關係人清楚傳達

上表所闡述的資料分析程式方法論只是一個起點，專家建議我們實地運用時別怕犯錯，並不斷微調架構，俾使此架構更臻周延，並時時更新紀錄風險、元資料及業務流程變更，當然也要時時留意未來資料分析者之出現，使之為自身所用。

講到這邊讀者也許覺得一切都太抽象了，所以接下來介紹來自美國奧勒岡州二名稽核人員親身經歷的有趣案例，他們分享運用科技進行資料爬梳的經過，並介紹了班佛定律(Benford’s law)的神奇測定功效，若仔細思考其資料爬梳經過，相信對於想牛刀小試資料分析稽核的讀者多少有點啟發。奧勒岡州如同美國其他各州有提供社會扶助補助，除了營養補給協助計畫、弱勢家庭暫時性急難救助等制度有漏洞，健保也有冒領問題存在。

奧勒岡州在分析州政府支出後發現 1/3 財政支出用於健保補助，於是決定深入分析資料了解真因，卻在分析後發現每月近 1 千萬美金係給付不合格的申請者，而系統控制阻止冒領及資料庫控制機制闕如，系統開發階段卻沒有相關測試及早偵知此漏洞，所以有 75%的健保給付欠缺稽核，經過資料比對結果，發現中樂透、退休者、監禁者、已死亡者等都在冒領之列，在被發現之前奧勒岡州的健保申請成長率名列第一，而該州也因發現此一漏洞而獲得國家表彰，但代價卻是幾千萬美金的損失，令人不勝唏噓。本制度的另一構面同樣發現有弊，也就是健保藥價冒領，該州透過分析發現尋常人一般由 2 位醫師開藥，並向 2 家藥局領藥，卻在分析資料庫後發現有 148 個人特別奇怪，由超過 30 位醫師開立處方，然後向超過 15 家藥局領藥，也就是典型的逛醫院病患(Doctor shopping)，經過歸納分析後發現其中牙醫佔了 72%最多，進一步分析後發現集中 5 名醫師協助開立處方，故事後續發展就請大家發揮想像空間囉。

另一個例子有關營養補助協助計畫，政府發放食物卡供民眾前往店家換取基本所需食物，在整併並交叉查詢政府各類資料庫後發現了驚人的事實，這裡面來申請補助的商家中有一家小型雜貨舖，客人平均每筆交易金額是 USD54，高於連鎖超商 7-11 的平均數，這種交易平均金額甚至高於 Walmarts 的平均數，進一步分析時發現其交易筆數比 Costco 還高，同張食物卡一天還有高達 500 筆的交易，由於資料顯示實在不尋常，調查人員甚至前往埋伏店家附近進行蒐證，蒐集客人進店消費時點、出店門時手提貨物與購買清單有出入等影像畫面，比如買了一大堆起司的顧客，卻兩手空空出店門，起司難道是藏在口袋裡? 而此類舞弊通常有個特徵，基於按耐不住慢慢賺的心理，每次交易金額會越來越高，譬如一般加油站平均消費金額是 USD4-8，但某犯案加油站的平均交易金額高達 USD35.36，比全國平均高出 534%，而聚焦該犯案店家的歷史紀錄，會發現每筆交易金額呈現與日俱增的趨勢，此外，班佛定律可以幫助你發現其中有詐，班佛定律說明一堆從實際生活得出的數據中，以 1 為首位數字的出現機率約為總數的三成，越大的數，以其為首幾位的數出現的機率就越低，亦即由 1 至 9 呈現一平滑下降曲線，它可用於檢查各種數據是否有造假。若有人為造假時，數字會說話，冒領者也許自己都沒發現，就是他們想出的交易金額數字多半都是 1 或 2 開頭，反而是 9 開頭的數字少很多，所以數據曲線就會脫離班佛定律曲線。但也是有很聰明的賊的，在 Arizona 州就發現 1 或 2 開頭的數字較少，反而是 8、9 開頭的數字開頭佔多數，明顯違反班佛定律的特徵也被抓出，因為還是不尋常的數字分布，大家或許不知道，班佛定律也是抓出安隆案作假帳的幕後功臣呢!奧勒岡州的稽核人員運用這些統計分析定律篩選過濾可疑店家後，再去各個調查擊破，最終起訴 5 個店家及 100 位顧客，成功追回 USD525,000，並避免了 1,600 萬美金的成本損失，奧勒岡州因此獲得聯邦政府 USD300,000 的獎勵。

兩位分享者最終的忠告很簡單，請各位同業隨時注意產業法令動態，那通常意味著最新風險趨向，而善用**大數據分析有助於快速找出潛在浪費、舞弊及濫用**，當然別忘了班佛定律，好好善用這工具可能會有意想不到的收穫喔!

(六)　舞弊偵防

舞弊案件曝光最常見原因為吹哨者舉報(佔 40%)，其次則是靠稽核人員發現異常現象(佔 15%)，經抽絲剝繭撞破舞弊手法。吹哨者舉報方面專家強調匿名熱

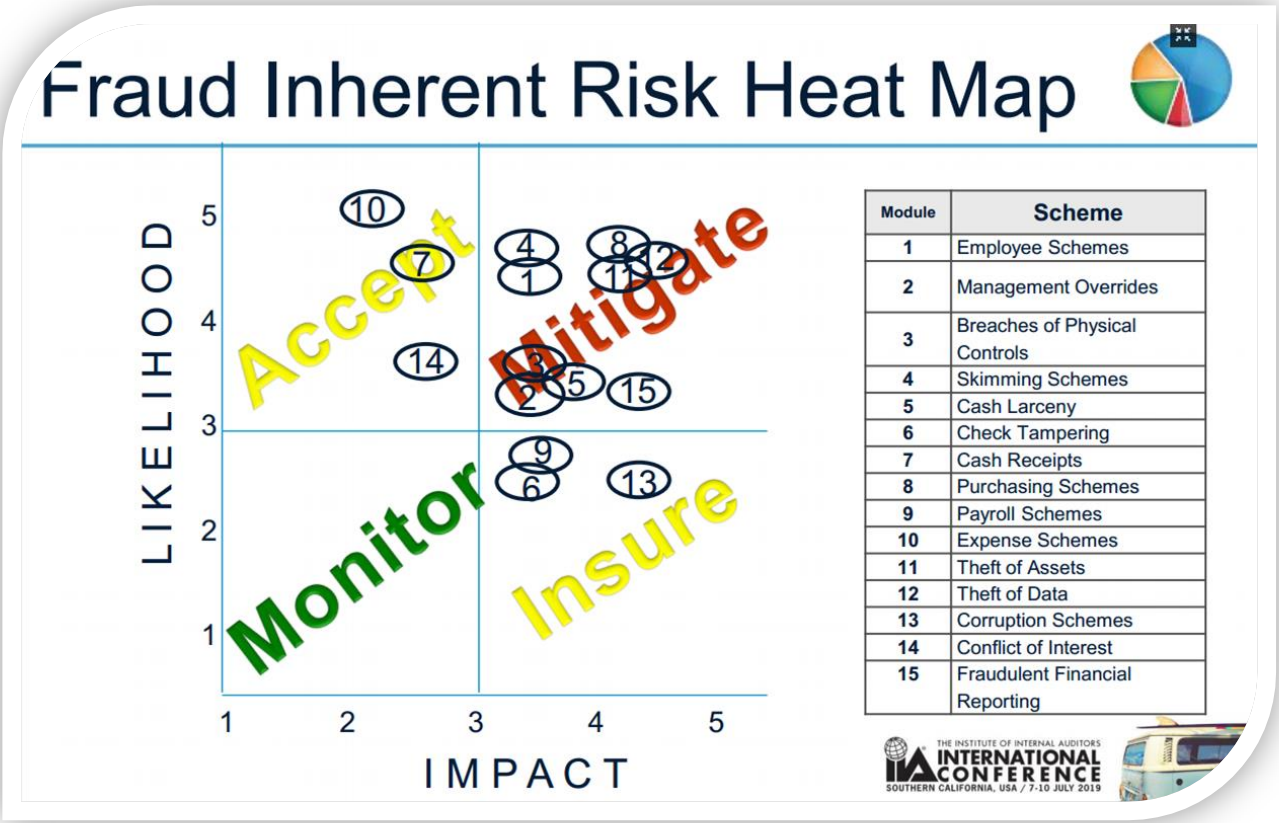
線設置的重要性，如何讓吹哨者能安心檢舉，不必擔心可能遭報復是此項功能存在的重要因素，也跟組織文化氣氛有關，**組織文化若沒有任何鼓勵勇於舉報違法行為，可能會錯失大部分阻止舞弊損失的機會**。根據統計發現，多數舞弊人員幾乎是初犯，而且組織損失數額隨共謀人數呈正比關係，專家建議透過以下方法，或可降低舞弊發生機率：

1. 上級支持
2. 職務分工
3. 持續性內部稽核
4. 突襲式稽核、交叉查核、外稽、董監事詳細詰問
5. 辨識並輪調流程關鍵點控制人員，減少形成共謀
6. 鉅細靡遺的分析(相關性分析)

一位銀行經理在舞弊防範意識上做了很好的示範，這位經理每天會抽查 5 張支票，簡單的舉動，雖然不見得會發現什麼問題，但每位行員都知道主管會抽查，小小舉動有效嚇阻舞弊發生的機率。此例顯示出舞弊防範無法單靠少數內稽人員努力，實有賴各級主管的重視及具體宣示性行動。

再談到異常現象調查，為了得到最佳解，稽核人員在偵蒐時需針對環境變數微調問題，查核過程或風險評估過程中可能會收集到一些文件，儘量從中獲取有用資訊，為了聚焦查核範圍此時會引入一些數據統計分析技巧，然後再跟當事人、利害關係人等求證資料正確性，並藉以拼湊未完備的事實真相。在蒐集到許多資訊後，下一步要去蕪存菁，過濾出有用的報告資料，所謂有用的資料通常可與「風險」相互連結，跟風險無關的雜訊毋需費力分析。

在舞弊預防上風險評估、風險庫分類等方式與一般年度稽核計畫風險評估方式極度類似，差別只在於範疇，舞弊風險評估排序、對應手法等會著重在人為舞弊熱點控制，而一般年度稽核計畫風險評估可能還包括環境風險等不可控風險控制部分，視可能性及衝擊度繪製風險圖像，分別採接受、減輕、監測、保險等對應手法如下圖。



針對各種舞弊風險進行權責部門分析、現有內控制度檢查、內控有效度評量（例示工具如下表），在檢視時也許就會發現內控不周延之處，透過填補內控漏洞增強風險控制，之後再檢視殘餘風險圖像以確定各類風險有降階趨勢。

Fraud Risk Scenario	Likelihood	Impact	Accountable Department	Existing Controls	Effectiveness of Controls	Policy & Procedures
Module #1						
Employee Schemes						
1.Employee's information used for hiring purposes is fraudulent increasing the risk of a bad hire. ***Risk*** Financial Reputational Operational Compliance	***Likely***	***Serious***	Human Resource Legal Finance	1. Dedicate professional recruiters 2. Existence of formal written job descriptions 3. Code of Ethics 4. Written fraud policy 5. Written policies and procedures 6. Integrity Hotline 7. Background check required for hire 8. Internal Audit Department 9. Automated timekeeping system to monitor vacation 10. Employees are adequately compensated	**Green**	C-100.10 Standards of Ethics and Business Conduct C-310.25 Fraud Waste & Abuse C-100.61 Integrity Hotline C-240.40 Vacation
1.Employees are not adequately trained to ensure acceptable behavior. ***Risk*** Reputational Operational Compliance	***Likely***	***Serious***	Human Resource	1. New employee orientation 2. New Manager training 3. Education University 4. Awareness intranet publications 5. Annual Conflict of Interest disclosure 6. Annual formal performance evaluations	**Yellow**	C-270.25 Staff Development and Mandatory Training C-270.30 Staff Orientation

三、 其他心得分享－個人風險管理

這次大會邀請到數名稽核界及其他領域成功人士前來分享成功的經驗，包含了資深演員、非裔古典鋼琴演奏家、地緣政治學者、聯合國世界糧食組織總稽核、美國眾議院總稽核、迪士尼前內部教練等，其中較令人印象深刻的幾位幾乎都具備跨界職涯發展，譬如《龐式騙局》演員 Richard Dreyfuss 除了是名得獎演員外，也自創非營利組織倡導言論自由、隱私權或民主等理念，他同時也擔任美國律師協會教育委員會成員等，另一位古典鋼琴演奏家則是同時身兼演說家及主持人，並致力於跨界音樂融合，將古典樂結合雷鬼音樂、rap 等，在她手中全都變成可能，並透過音樂創意混搭刺激各種領域聽眾勇於接受挑戰及改變，並致力於提升自身的多樣性，她跨出了古典樂界，讓自己受邀於各種不可能的場合表演及演說，這些講者讓我們觀察到斜槓的趨勢，進一步思考後筆者推斷出這種趨勢來自於個人面對職涯風險時不得不作出的改變，若從事某種單一領域，該領域面臨極度不穩定的工作來源時，**多能工**應運而生，許多多能工並非做好充足準備才跨界，而是在被迫跨界過程中鍛鍊新技能，現今世代專業職人工作機會在減少，因為除了高階專業工作(醫生、晶片設計師等)外，其他各類工作都可能被人工智慧或電腦取代，於是復古多能工再度流行，其實這並不是不可能，看看達文西、亞里斯多德、春秋時代范蠡、東漢張衡等，這些古代偉人其實都是多才多藝的代表，也許是時勢所逼，卻能更增添個人生涯風險承受復原力，當其他人只能賺單一財時，這些人開拓了職涯可能，賺起跨界財，所以這些成功人士帶來的啟發就是擁抱改變，擁抱改變才是多樣性培養的起點。其中還有一位未來家(futurist)跟大家分享了未來 AI 世界的輪廓，並對個人、領導者等提出了思維模式調整忠告，包括了自我思考挑戰、汲取團隊中年輕成員觀點、擁抱大數據創價文化、結合 AI 的迅捷團隊組織型態崛起等，看看這些建議，也許還是要從擁抱改變做起。

肆、 結論與建議

本報告中介紹稽核作業各階段可運用之工具，建議讀者可從資料分析、班佛定律等較易執行之工具入門試作，完成資料蒐集後自我檢視是否曾犯各類判斷偏

誤，修正判斷標準避免再犯，而隨經驗增加後再漸進導入其餘各類環境監控、第三方管理等結構性構面檢視，俾使稽核構面更臻周延。參加本次國際稽核研討會各個場次均能發現風險評估及管理的蹤影，顯示稽核領域工作仍首重了解企業風險，若未在一開始即釐清風險趨向或所在，則後續開展再多稽核工作或內部控制設計只會事倍功半，遑論稽核技巧應用等管末技術精進之效果，組織各階層工作人員不知為何而忙，稽核工作者則是矇著眼睛亂槍打鳥，欠缺方向性的內控工作最終仍禁不起環境或市場風險打擊，驀然回首眾人不解為何傾盡全力仍會失敗，亦無從得知失敗根因，其實是整體系統性失靈導致，難以歸咎單一事件或因素。許多**企業辦理年度風險辨識、評估、控管工作時淪為紙上談兵、例行公事，大多數工作人員大費周章盲目「填表」好交差了事**，或拘泥於格式不符、或受現有內控制度限制思考，**時常拿出去年表件複製貼上，好似經營環境、業務變化一成不變**，如何喚醒組織全員清醒進行風險評估，確實是大象型企業最難克服的任務。建議須先喚醒各級主管風險意識，配合貫徹風險管理精神，內部稽核工作者則是在進行各單位年度實地查核時強化風險意識，利用訪談詢問了解基層人員對於風險管理的認識程度，透過稽核方向誘導各級重新思考辦理風險評估及管理的意義，也透過改善建議去矯正錯誤的觀念，如此才能持續維持組織生於憂患的經營精神。

這次研討會也提及另一個容易受人忽略或抑制發揮的內部稽核功能，內部稽核由於稽核範疇遍及全公司業務，**就各單位遭遇之業務困境有時能提供諮詢功能**，類似他山之石可以攻錯的概念，尤有甚者對於制度運作稍有了解者還能提供跨單位建議解決方案，然而在不得犯錯及階級分明的東方文化薰陶下，此種功能受到抑制，為免得罪各方山頭、無事生事或恐誤判情勢提出錯誤見解，多數人選擇沉默是金，西方組織容許犯錯、勇於表達自我意見的文化氛圍下，則較能受惠內部稽核的諮詢功能，然而筆者仍在許多小地方看見稽核人員默默發揮這項功能，在實地查核過程中扶助單位解決困難、提高工作效率，這是稽核這項工作振奮人心之處，雖然時常遭人嫌棄，這群企業啄木鳥依然默默的堅持在工作崗位上，稽核的諮詢角色最能代表這份工作的價值，與所有稽核同袍們共勉。